(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/015043 A1

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/GB02/03485

(22) International Filing Date: 29 July 2002 (29.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0119040.4 3 August 2001 (03.08.2001) GB
PCT/GB01/04072 11 September 2001 (11.09.2001) GB

(71) Applicant *(for all designated States except US)*: HALTFERN LIMITED [GB/GB]; 2 Mountview Court, 310 Friern Barnet Lane, Whetstone, London N20 0YZ (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: CODRON, Izidore [IT/ZA]; No 1 Cassell Road, Sea Point, 8005, Cape Town (ZA).

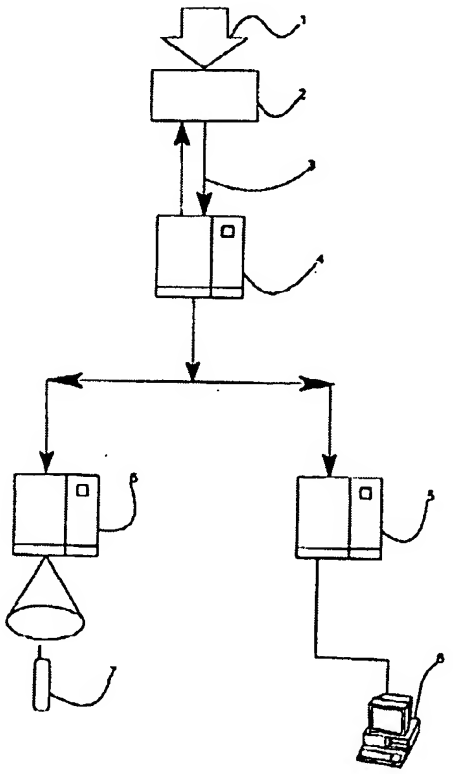
(74) Agent: KEMP, Paul, Geoffrey; Brookes Batchellor, 102-108 Clerkenwell Road, London EC1M 5SA (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK,

[Continued on next page]

(54) Title: A CREDIT CARD SECURITY SYSTEM



(57) Abstract: The specification discloses a credit card security system in which a security server (4) is arranged to respond to the initiation of a transaction (1) by instantly transmitting an SMS text message to the credit card holder's cellular mobile phone (7).

WO 03/015043 A1

TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A Credit Card Security System.

The present invention is concerned with a credit card security system which is able to reduce the fraudulent use of a card.

The problem of fraudulent use of a credit card will be familiar to most and is becoming more serious as credit card and like transactions become more commonplace. A frequent problem results from a credit card or card data being stolen and used fraudulently for hours or even days, while the card holder is unaware of the abuse and so unable to alert the card issuer.

In the ordinary course of implementing a credit card transaction it is commonplace that the transaction will be recorded immediately to a server, if the transaction takes place in a conventional shop this is usually achieved by swiping the card through a transaction machine and the machine then addresses a remote card credit checking server provided by the credit card issuer and interrogates a database in the remote credit checking server for credit worthiness. The credit checking server will then respond by issuing signals to the transaction machine either approving the transaction or rejecting the transaction. In the case of remote transactions, it is usual that the credit card details are logged directly to a vendor's in house transaction system, either manually if the transaction is a telephone sale or directly if the sale is via the world wide web. The present invention seeks to take advantage of the existing system of processing credit card transactions and so improve credit card security at minimal cost

Accordingly the present invention provides a credit card security system having:

a credit card bearing data corresponding to a card holder account

a security server arranged to receive said card holder account data when a credit card account transaction is initiated and responsive to receipt of said data to transmit a message immediately to at least one of a mobile phone account in the name of said card holder or an email account in the name of said cardholder.

According to a second aspect of the present invention there is provided a method of improved credit card security comprising the steps of:

initiating a transaction by communicating data corresponding to a card holder account to a vendor,

said vendor communicating said card holder account data to a security server,

said security server responding to said credit card holder account data by addressing at least one of mobile phone account data or email account data previously provided by the credit card holder, and sending at least one of an SMS message or email to said mobile phone or email account.

By immediately transmitting a message to the legitimate card holder's mobile phone and/or email account the legitimate card holder is immediately (often in a period of less than 30 seconds and usually less than 300 seconds) warned that use is being made of his card. By conventional means the credit card user may be unaware of the abuse of his card until he receives the monthly card balance probably days or weeks later, even then the abuse may not be instantly obvious. Thus the present invention gives a clear and immediate warning if the credit card account is being used fraudulently and this will give the legitimate card holder a very early opportunity to alert the credit card provider to the fraudulent use so that steps can be taken to prevent further abuse.

The mobile phone account data and/or email account data may be presented on the card in which case it is preferable that the data is encrypted and in machine readable form, such as the conventional magnetic strip or electronic memory. However, it is preferred that the credit card provider pre-loads the mobile phone and/or email account data onto the security server. The credit checking server or a server in close communication with the credit checking server may conveniently serve as the credit checking server. In this way the mobile phone data and email account data is not available to a thief and the mobile phone and email data can be readily managed by the credit card provider in cooperation with the credit checking service provider. In this

preferred embodiment of the invention the security server has means to receive said card holder account data when a credit card account transaction is initiated, memory means which holds card holder account data, and memory means holding at least one of mobile phone account data or email account data. The security server is responsive to receipt of said card holder account data to recover at least one of the mobile phone account data or email account data corresponding to said card holder account data received from memory and has transmission means to transmit a message immediately to at least one of the mobile phone account or email account corresponding to said card holder.

It is preferred that the message is a text message.

The security system and method may be further enhanced by enabling the card holder's mobile phone to respond to the message with a default stop or proceed message to stop or expedite the transaction. A stop message might then be retransmitted from the security server to the vendor so that if the transaction is fraudulent the transaction can be stopped by the vendor. Preferably the mobile phone would be adapted to present the message in a way which allows the credit card holder to respond to the message from a soft key, selecting proceed or stop, alternatively one or two of the phone keys may be used to transmit a default, proceed or stop message to the security server. The security system may be set to allow a transaction to proceed if no response is received from the mobile phone within a predetermined period, for example, ninety seconds. This will allow transactions to proceed where the mobile phone is out of service for any reason.

Embodiments of a credit card security system constructed and operated according to the system and method of the present invention will now be describe, by way of example only, with reference to the accompanying illustrative drawings, in which:

Figure 1 is a first embodiment of the system, and

Figure 2 is a second embodiment of the invention.

Figure 1 shows a credit card transaction being implemented using the security system. At 1 data indicative of the credit card account is input to a vendor's transaction computer/server 2. The data input may be via a card reader, by manual input, direct input via internet access or by any other conventional means. This data is processed in the usual way and communicated via normal telecommunication 3 to security server provided in this example by a card credit checking server 4 in two way communication with the vendors server 2. The card credit checking server 4 includes a register of email addresses and cellular mobile phone numbers which correspond to each credit card account. Upon receipt of the credit card account data the card credit checking server addresses the corresponding mobile phone account number and/or email address and forwards a predetermined message to an internet server 5 and/or a cellular network server 6 and hence to the credit card holder's mobile phone 7 or computer 8. The message will preferably be a text message and may in addition to an indication that a transaction has been implemented include further information data such as the location, time and value of the transaction. Particularly if this further information is delivered to a PC or other handheld type device this will allow credit card holders to maintain nearly instant monitoring of their credit card account balance in addition to enhancing the security of the account.

Although this specification refers particularly to credit cards, it should be appreciated that the term credit card may also include debit cards and other forms of payment card, including; smart cards, stored value cards and any other microprocessor payment system embedded in hand held devices like mobile phones or personal digital assistants (PDA's). These chip cards will have a processor, ROM and RAM, an operating system and even co-processor power for handling Crypto Algorithms in real time allowing the card or handheld device to trust or distrust a terminal on or off-line. Such a terminal will have the ability to intelligently interrogate a payment card or hand held device micro-processor payment system and locally satisfy itself that the card is

trustworthy. It may also have application where card like devices are used in smart security systems as a key to provide access to restricted areas, in such instances the unauthorised use of an authorised key would be alerted to the authorised user.

Figure 2 diagrammatically illustrates a second embodiment of the invention. The components of the system common to the first embodiment are similarly numbered and only the differences between the two embodiments will be described. When the security server 6 generates a message to the mobile phone 7a the message includes code to generate one of two response messages from the phone. Thus when a message such as that illustrated on the phone display is received it includes that the message is a "credit card transaction alert" here abbreviated to "CC TRNS ALT" the date and time and the location "@XXXXXXX" there is additionally a question "PROCEED?" 9. The message establishes a softkey 9 option "YES" to respond with a proceed message and option "NO" to respond with a stop message. In the figure, "NO" is selected which message 10 is transmitted to the cellular network server 6. The message from the phone will include code to identify the phone. This is then retransmitted to the card credit checking and security server 4 which matches the phone to the transaction in issue by correlation with a register of mobile phone account data. Thus a stop message reaches the vendor's transaction server 2 where steps may be implemented in a conventional manner to stop the transaction. The security server 4 will ordinarily wait for a period, for example ninety seconds, before emitting a proceed message based on conventional card credit criteria. Thus the proceed message may expedite a transaction. Conversely a stop message from the mobile phone or any stop transaction message based on other criteria will take priority.

Claims

1. A credit card security system having:

a credit card bearing data corresponding to a card holder account

a security server arranged to receive said card holder data when a credit transaction is requested and responsive to receipt of said data to transmit a message immediately to at least one of a mobile phone account corresponding to said card holder or an email account in the name of said cardholder.

2. A credit card security system according to claim 1 wherein the security server has;

means to receive said card holder account data when a credit card account transaction is initiated, and

memory means holding at least one of mobile phone account data or email account data addressed according to the card holder account data,

said security server being responsive to receipt of said card holder account data to recover at least one of the mobile phone account data or email account data corresponding to said card holder account data received and having

transmission means to transmit a message immediately to at least one of the mobile phone account or email account corresponding to said card holder.

3. A credit card security system according to claim 1 or claim 2 wherein the security server is provided by the credit card issuer.

4. A credit card security system according to any one of the preceding claims wherein the security server is downstream of a vendor's transaction server to receive the account data from the vendor's transaction server.

5. A credit card security system according to claim 4 wherein the security server is provided by a card credit checking server.

6. A credit card security system according to claim 1 wherein the credit card holder's mobile phone account number or email address are encoded on the credit card and the data is recoverable from the card when the card is swiped in a transaction machine by a vendor to be used by the security server in communication with the transaction machine to transmit the message.

7. A credit card security system according to any one of the preceding claims wherein the security server has means to receive a predetermined stop message from the mobile phone encoded to indicate that the transaction should be stopped.

8. A credit card security system according to claim 7 wherein the security server has means adapted to respond to receipt of a predetermined stop message to transmit a message to the vendor to stop the transaction.

9. A credit card security system according to claim 7 or 8 wherein the security server has means to receive a predetermined message from the mobile phone to indicate that the transaction should proceed, and means adapted to respond to receipt of the proceed message to send a proceed message to the vendor.

10. A method for improving credit card security when a card transaction is initiated comprising the steps of:

a card holder communicating data corresponding to a card holder account to a vendor,

said vendor communicating said data to a security server,

said security server responding to said credit card holder account data by addressing at least one of mobile phone account data or email account data corresponding to said card holder account and previously provided by the credit card holder, and sending one of an SMS message or email to said mobile phone or email account.

11. A method according to claim 10 comprising the step of the credit card issuer providing the security server.

12. A method according to either one of claims 10 or 11 wherein said security server responding to a predetermined stop message from the account holder's mobile phone by transmitting a stop message to the vendor to stop the transaction.

13. A method according to any one of claims 10 to 12 wherein the security server mobile phone is adapted to send a proceed message to the security server in response to the transaction message, said server responding by transmitting a proceed message to the vendor.

14. A method according to claim 10 wherein the mobile phone data or email data is encrypted on the credit card and comprising the step of the data being read from the credit card when the credit card is swiped in a transaction machine provided by a vendor,

said transaction machine communicating said mobile phone or email data to a server,

said server communicating an SMS message or email to the address of the credit card holder.

15. A server adapted to receive data identifying a credit card account, said server having a register preloaded with a mobile phone account number and/or email address corresponding to the holder of the credit card account, said server being adapted to respond to data indicating that a transaction is to be implemented using said credit card account by recovering a mobile phone and/or email address corresponding to the credit card account and said server being provided with communication means to issue a message to said mobile phone account or email address.

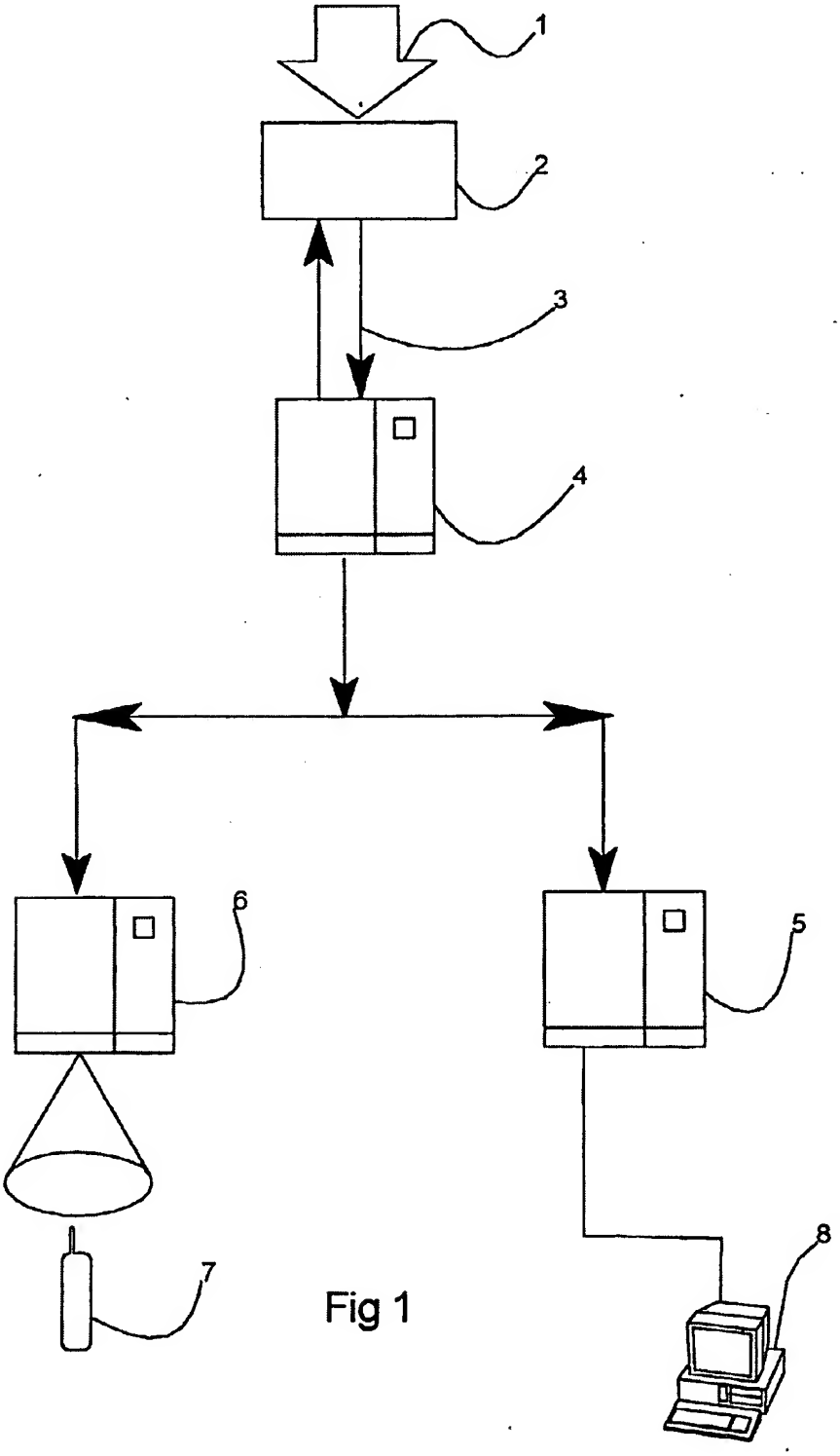


Fig 1

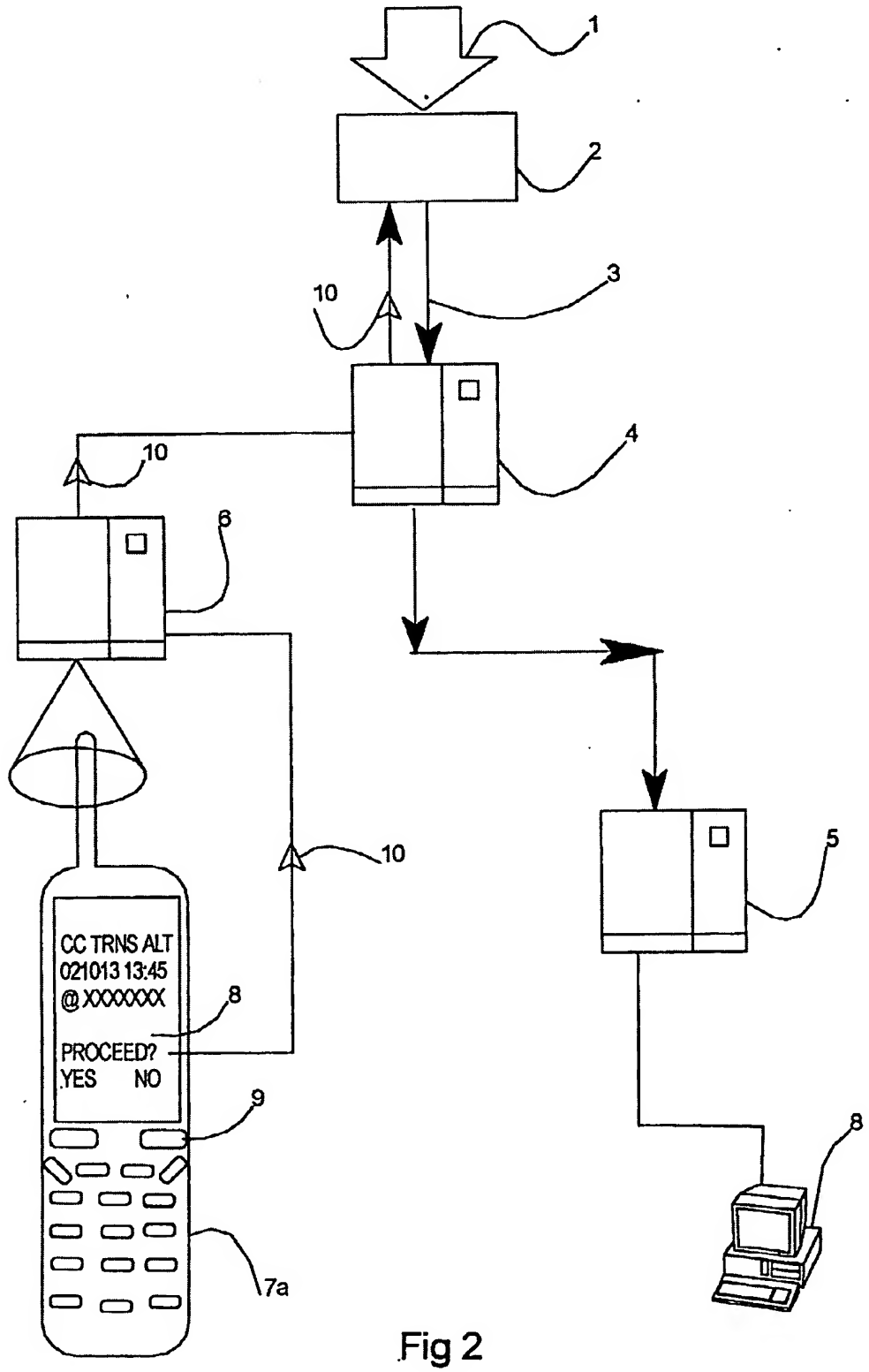

1
2
3
10
4
10
6
10
5
CC TRNS ALT
021013 13:45
@XXXXXXX
PROCEED?
YES NO
8
9
7a
8

Fig 2

INTERNATIONAL SEARCH REPORT

PCT/GB 02/03485

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 55984 A (BADENHORST CORNELIUS JOHANNES ;FUNDAMO PROPRIETARY LTD (ZA); RENSB) 2 August 2001 (2001-08-02)	1
A	abstract page 5, column 20-30; figure 1	2,10,15
X	WO 01 52205 A (SEAGLADE DEVELOPMENTS LTD ;MEAGHER PHILIP (IE)) 19 July 2001 (2001-07-19)	1-5, 7-13,15
Y	abstract; figure 2 page 11, line 1 -page 12, line 22; claim 1 page 3, line 31 -page 4, line 2	6,14
X	FR 2 801 995 A (DUVAL BRUNO) 8 June 2001 (2001-06-08)	1-5, 7-13,15
	abstract; claim 1; figures 1,2	
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 October 2002	23/10/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Laub, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

PCT/GB 02/03485

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 065 634 A (MIC SYSTEMS) 3 January 2001 (2001-01-03) abstract; figure 2A	1-15
Y	EP 0 793 206 A (HITACHI LTD) 3 September 1997 (1997-09-03) column 3, line 33-36; figure 16	6,14
A	WO 01 01300 A (HILSON DANIEL ANDREW ;INDUSTRY WIDE NETWORKS PTY LTD (AU)) 4 January 2001 (2001-01-04) page 10, line 38 -page 11, line 10	1,10,15

INTERNATIONAL SEARCH REPORT

Information on patent family members

PCT/GB 02/03485

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0155984 A	02-08-2001	AU 2699601 A	07-08-2001
		AU 2872801 A	07-08-2001
		AU 2873001 A	07-08-2001
		AU 3042701 A	07-08-2001
		AU 3042801 A	07-08-2001
		EP 1245011 A1	02-10-2002
		WO 0155982 A1	02-08-2001
		WO 0155983 A1	02-08-2001
		WO 0155984 A1	02-08-2001
		WO 0155981 A1	02-08-2001
		WO 0155921 A1	02-08-2001
WO 0152205 A	19-07-2001	AU 2700701 A	24-07-2001
		WO 0152205 A1	19-07-2001
FR 2801995 A	08-06-2001	FR 2801995 A1	08-06-2001
		AU 2525001 A	18-06-2001
		WO 0143092 A1	14-06-2001
EP 1065634 A	03-01-2001	EP 1065634 A1	03-01-2001
		AU 6268300 A	22-01-2001
		WO 0103083 A1	11-01-2001
EP 0793206 A	03-09-1997	CA 2197933 A1	29-08-1997
		EP 0793206 A2	03-09-1997
		JP 9307660 A	28-11-1997
WO 0101300 A	04-01-2001	WO 0101300 A1	04-01-2001
		AU 6139100 A	31-01-2001